THE ANONYMOUS POSTER: HOW TO PROTECT INTERNET USERS' PRIVACY AND PREVENT ABUSE

SCOTT NESS[1]

ABSTRACT

The threat of anonymous Internet posting to individual privacy has been met with congressional and judicial indecisiveness. Part of the problem stems from the inherent conflict between punishing those who disrespect one's privacy by placing a burden on the individual websites and continuing to support the Internet's development. Additionally, assigning traditional tort liability is problematic as the defendant enjoys an expectation of privacy as well, creating difficulty in securing the necessary information to proceed with legal action. One solution to resolving invasion of privacy disputes involves a uniform identification verification program that ensures user confidentiality while promoting accountability for malicious behavior.

INTRODUCTION

¶1 The right to privacy is not derived from any single source. The Universal Declaration of Human Rights recognizes that "[no] one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his [honor] and reputation."[2] Europeans have long adhered to a similar agreement, which promotes individual privacy.[3]

---

[1] JD Candidate at Duke University School of Law, 2011; B.A. in History from Haverford College, 2008. The author would like to thank Professor G. William Brown, Duke University School of Law, for his invaluable guidance with this iBrief, as well as friends and family for their support. Any errors within this iBrief are solely those of the author.

[2] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) [hereinafter *UDHR*], *available at* http://www.un.org/en/documents/udhr/("[Everyone] has the right to the protection of the law against such interference or attacks."). The General Assembly adopted the UDHR as a "common standard" for recognizing the "equal and inalienable" rights of all humans, "the foundation of freedom, justice and peace in the world." *Id.*

[3] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8(1), Nov. 4, 1950, 213 U.N.T.S. 221 (entered into force Sept. 3,

¶2 More recently, the right to privacy is protected by the Privacy Act of 1974.[4] The United States Constitution does not explicitly mention a right to privacy; the Supreme Court, however, has found a right to privacy implicit within the First, Third, Fourth and Fifth Amendments.[5]

¶3 The right to privacy in the U.S. traces its roots to an 1890 article written by Samuel D. Warren and Louis D. Brandeis.[6] In that article, Warren and Brandeis outlined a basis for receiving compensation from the tort of invasion of privacy.[7] Within the spectrum of invasion of privacy are three subcategories particularly relevant when confronting Internet exposure. First, public disclosure of private facts constitutes a tort if both parties believe that the embarrassing matter is true and the plaintiff's injury resulted from that assumption.[8] Second, publicly publishing a matter concerning another individual in a false light implicates invasion of privacy tort liability.[9] Finally, an invasion of privacy claim is available in cases where a plaintiff's name or likeness is appropriated for the benefit of another. [10]

¶4 The threat of technological advances to individual privacy has been met with congressional indecisiveness. Congressional action to impede digital invasions of privacy—like the Electronic Communications Privacy

---

1953) ("Everyone has the right to respect for his private and family life, his home and his correspondence."), *available at* http://www.pfc.org.uk/node/328.

[4] 5 U.S.C. 552a(b) (1974) ("No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.").

[5] Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (citations omitted) ("[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. . . . [America has] had many controversies over these penumbral rights of 'privacy and repose.' These cases bear witness that the right of privacy which presses for recognition here is a legitimate one.").

[6] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[7] *Id.* at 213 ("If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.").

[8] DAVID A. ELDER, PRIVACY TORTS § 3:1 (2009).

[9] *See* RESTATEMENT (SECOND) OF TORTS § 652E (1977). Plaintiffs seeking damages for false light invasion of privacy claims must also show that the false light in which the defendant cast the plaintiff would be "highly offensive to a reasonable person," and that the defendant had knowledge of or acted in reckless disregard as to the falsity of the publicized matter. *Id.*

[10] *Id.* § 652C.

Act (ECPA)[11]—has been stymied by its conflicting goal of supporting the Internet's development. Indeed, this goal is featured prominently in the Communications Decency Act of 1996 (CDA),[12] in which Congress recognized that "the United States [should] promote the continued development of the Internet and other interactive computer services and other interactive media."[13] Fueled by this desire to empower web-based companies, Congress included a "Good Samaritan" clause in the CDA. The clause absolves interactive service providers of civil publisher or speaker liability so long as the service provider acts in good faith to restrict access to damaging material.[14]

¶5 One of the most prominent characteristics of the internet is anonymity. Anonymous posting is now in vogue, with the advent of College Anonymous Confession Board (CollegeACB).[15] CollegeACB intends to "[help] build community and [engender] the open exchange of information."[16] The site, however, is the successor to the notorious JuicyCampus,[17] a website that reveled in salacious posts.[18] JuicyCampus's scandalous posts dried up after students "spammed" the site with random book excerpts, biblical quotes, and poetry verses.[19] The lack of participation by the courts in JuicyCampus's shutdown demonstrated judicial unwillingness to act against Internet entities, even when violations of privacy rights were blatant.[20]

---

[11] 18 U.S.C. §§ 2510–22 (2006). Section 2511 establishes criminal liability for one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."

[12] Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 133–43 (1996) (codified in scattered sections of 47 U.S.C.).

[13] 47 U.S.C. § 230(b)(1) (2006).

[14] *Id.* § 230(c).

[15] College Anonymous Confession Board Home Page, http://www.collegeacb.com/ (last visited Mar. 31, 2010)

[16] CollegeACB,. Press Release. (Feb. 5, 2009), *available at* http://collegeacb.blogspot.com/2009/02/collegeacb-press-release.html (last visited Mar, 31, 2010).

[17] JuicyCampus, http://juicycampus.blogspot.com/ (last visited Mar. 31, 2010).

[18] *Id. See also* Jeffrey R. Young, *JuicyCampus Shuts Down, Blaming the Economy, Not the Controversy*, CHRON. HIGHER EDUC. (D.C.), Feb. 5, 2009, http://chronicle.com/article/JuicyCampus-Shuts-Down-Bla/1506/ (explaining that the site openly encouraged salacious postings through its motto "Keep it Juicy").

[19] Jessica Bell, *Students 'Spam' JuicyCampus*, DAILY PENNSYLVANIAN, Oct. 31, 2008, http://thedp.com/node/57393.

[20] See discussion *infra* ¶¶ 29-30 for a more in-depth discussion of the JuicyCampus case.

¶6 Part I of this iBrief describes the tort of invasion of privacy, its formulation and the elements required to plead a viable claim. Part II evaluates the ECPA and its application within the Internet context. Part III discusses the goals of the CDA and the legislative history behind the act and the controversial "Good Samaritan" provision. Part IV considers the privacy issues associated with Internet anonymity.

¶7 Part V examines how, while courts are mindful of the disintegrating privacy boundaries in cyberspace, they nevertheless refuse to allow actions against the sites that encourage such behavior because they continue to abide by the principles set forth in the CDA and strive to promote the perpetual growth of the Internet.[21] On the other hand, courts have imposed injunctions against sites where the entity's positive contributions to Internet usage cannot outweigh the negative goal the site furthers and the resultant public outcry for harsh action, such as Napster.[22]

¶8 Faced with this disheartening judicial inconsistency, Part VI describes one possible solution: a uniform identification verification program similar to VeriSign, but with statutorily mandated confidentiality that can only be abrogated after meeting a high burden of proof of harm. Such a program would guard free speech, promote accountability for malicious actions of bloggers and anonymous posters, and still permit websites to operate and innovate.

I. THE TORT OF INVASION OF PRIVACY

¶9 The tort of invasion of privacy finds its origins in Samuel Warren and Louis Brandeis's "The Right to Privacy," in which the authors recognized that an individual should have full protection in person and property. [23] Known as the "inviolate personality," this concept has existed as long as the Common Law.[24]

¶10 At the turn of the twentieth century, "instantaneous photograph and newspaper [enterprises]" thrived on sensationalism; they repeatedly demonstrated a lack of consideration for "the obvious bounds of propriety and of decency."[25] Thus, it became necessary for individuals to find "some retreat from the world."[26] The remedies for such a violation would likely be

---

[21] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).
[22] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).
[23] Warren & Brandeis, *supra* note 6, at 205.
[24] *Id.* at 193.
[25] *Id.* at 195–96; *see also* ELDER, *supra* note 8, at § 1:1 (expanding on Warren and Brandeis's discussion of the "yellow-journalism" press's willingness to dismiss individual privacy).
[26] Warren & Brandeis, supra note 6, at 196.

damages or an injunction, though the latter's applicability would be very limited.[27]

¶11 Following the Warren and Brandeis article, the legal community took notice of tort liability involving privacy issues. In 1960, William Prosser conceived the modern framework for privacy torts and articulated four categories under which a claim could be brought: intrusion upon seclusion, public disclosure, false light, and appropriation.[28] For the purpose of evaluating Internet claims, this iBrief only concerns itself with public disclosure, false light, and appropriation.

¶12 Under the Prosserian model, a public disclosure entails "publicity to a matter concerning the private life of another, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[29] It is not sufficient to disclose private information to a single individual or a small group of people.[30] In cases where all parties believed the revealed material to be true at the time of the disclosure and subsequent injury resulted from an assumption of truthfulness, a later discovery that the information was inaccurate does not preclude the disclosure action.[31]

¶13 Under the standards outlined by the American Law Institute, a defendant who publicizes a matter concerning another that places the other in a false light is subject to liability to the other for invasion of his privacy, if the false light in which the other was placed would be offensive to a reasonable person.[32] False light claims require that "the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[33] The reasonable person standard regarding offensiveness is crucial in these cases as inaccurate statements, though undesirable, are commonplace.[34]

---

[27] *Id.* at 219.

[28] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960). These types of invasions were to be viewed as distinct as they "may be subject, in some respects at least, to different rules; and that when what is said as to any one of them is carried over to another, it may not be at all applicable, and confusion may follow." *Id.* The American Law Institute incorporated the Prosser framework into the Second Restatement in 1979. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[29] RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[30] *Id.*

[31] ELDER, *supra* note 8, § 3:1.

[32] RESTATEMENT (SECOND) OF TORTS § 652E (1977).

[33] *Id.*

[34] *See id.* cmt. c ("Complete and perfect accuracy in published reports concerning any individual is seldom attainable by any reasonable effort, and most minor errors, such as a wrong address for his home, or a mistake in the

Though false light and defamation claims are quite similar, the conduct actionable under this claim is not necessarily defamatory in nature, and courts finding a false statement or impression not defamatory are not precluded from imposing liability for false light.[35]

¶14 Finally, an invasion of privacy claim is available against one who appropriates to his own use or benefit the name or likeness of another.[36] This form of invasion of privacy is commonly claimed when the defendant uses the plaintiff's identity to promote a business or product.[37] It is not enough that the defendant uses the plaintiff's name or identity as the defendant must adopt it for its potential benefit or value.[38]

II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

¶15 The Electronic Communications Privacy Act (ECPA)[39] contains the Wiretap Act[40] and the Stored Communications Act.[41] Title I of the ECPA amends the Federal Wiretap Act,[42] addressing the problem of unwanted interception of wire, oral and electronic communications.[43] Title II, the Stored Communications Act, focuses on the security of stored communication from dissemination or review.[44]

¶16 The ECPA regulates the circumstances under which electronic communications may be reviewed by third parties, including Internet service providers (ISPs). Under the ECPA, it is illegal to intercept or procure any electronic communications, unless various exceptions apply.[45] Such exceptions include (1) service of a court order;[46] (2) the content of the

---

date when he entered his employment or similar unimportant details of his career, would not in the absence of special circumstances give any serious offense to a reasonable person. The plaintiff's privacy is not invaded when the unimportant false statements are made, even when they are made deliberately.").

[35] ELDER, *supra* note 8, § 4:1.

[36] RESTATEMENT (SECOND) OF TORTS § 652C (1977).

[37] *Id.* § 652C, cmt. b.

[38] *Id.* § 652C, cmt. c (explaining that the defendant must have also appropriated the plaintiff's reputation, prestige, social standing or other public interest).

[39] 18 U.S.C. §§ 2510–2522 (2006).

[40] *Id.*

[41] *Id.* §§ 2701–2712. The Stored Communications Act is the ECPA section most applicable in Internet privacy litigation.

[42] 18 U.S.C. § 2510, *et seq*.

[43] S. REP. NO. 99-341, at 1–3 (1986).

[44] *Id.* at 3.

[45] 18 U.S.C. § 2511(1)(a). "Electronic communications" include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." § 2510(12).

[46] *Id*. § 2511(2)(a)(ii)(A).

electronic communication is readily accessible to the general public;[47] or (3) the communication is inadvertently obtained by the service provider, and its content pertained to criminal activity and is made available to law enforcement officials.[48]

¶17 The Stored Communications Act provides that it is illegal to obtain, alter, or otherwise interfere with authorized access to a wire or electronic communication while it is in electronic storage by intentionally accessing without authorization, or exceeding one's authorized access to, a facility through which an electronic communication service is provided.[49] The provisions within the Stored Communications Act do not apply in cases where the conduct in question was authorized by the person or entity providing the wire or electronic communications service, or alternatively by a user of that service with respect to a communication of or intended by that user.[50]

¶18 In one of the early Internet privacy cases to employ the ECPA, a group of internet users mounted a class action against DoubleClick, Inc.[51] The plaintiffs claimed that DoubleClick, an Internet advertising service, had inserted cookies[52] on users' computers and collected private information, including names, e-mail addresses, home and business addresses, telephone numbers, individual's Internet history including prior web searches and sites visited, and other communication and additional data that Internet users would not ordinarily expect advertisers to be able to collect.[53] The plaintiffs asserted that the placement of cookies on their hard drives constituted an unauthorized access and, as a result, violated Title II of the ECPA.[54]

¶19 The Court rejected the ECPA claim, noting that the cookies were not intended to be temporary, and therefore did not fall within the statutory

---

[47] *Id.* § 2511(2)(g)(i).
[48] *Id*. § 2511(3)(b)(4).
[49] *Id.*§ 2701(a) (2006).
[50] *Id.* § 2701(c).
[51] *In re* DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001). The plaintiffs claimed that DoubleClick had violated the ECPA as well as the Computer Fraud and Abuse Act, 18 U.S.C. 1030, *et seq.*, and raised several New York state common laws claims, including invasion of privacy, unjust enrichment, and trespass to property. *Id.*
[52] "Cookies" are defined in this case as "computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner." *Id.* at 502–03.
[53] *Id.* at 503.
[54] *DoubleClick*, 154 F. Supp. 2d at 507.

framework of Title II.[55] Furthermore, even if the cookies and their identification numbers were electronic communications in electronic storage, DoubleClick's access was still authorized as Title II exempted conduct, which was authorized by a user of the service with respect to a communication of or intended for that user.[56] The court concluded that the cookies' identification numbers were in fact internal DoubleClick Communications, "of" and "intended for" the company.[57]

¶20 The technical complexities involved in *DoubleClick* illuminate the challenges faced by courts applying existing law to cyberspace. Here, the *DoubleClick* court is quite competent in articulating Internet structure and programming.[58] However, Tasker and Pakcyk suggest that attorneys and judges do not necessarily possess the proper insight into the legal ramifications related to computer programming and processes.[59] For this reason, the effectiveness of the ECPA remains in doubt.

III. THE COMMUNICATIONS DECENCY ACT OF 1996

¶21 Congress formulated the CDA to expand upon the nation's policy of promoting the continued development of the Internet,[60] and maintaining the "vibrant and competitive free market" for web-based products and services.[61]

---

[55] *Id.* at 512 ("Title II only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it.")

[56] *Id.* at 513; *see* 18 U.S.C. § 2701(c)(2).

[57] *DoubleClick*, 154 F. Supp. 2d at 513 ("DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs' hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. In contrast, virtually all plaintiffs are unaware that the cookies exist, that these cookies have identification numbers, that DoubleClick accesses these identification numbers and that these numbers are critical to DoubleClick's operations.").

[58] *See id*. at 503–05 (explaining how DoubleClick targets banner advertisements and utilizes cookies to collect user information); *see also* Ty Tasker & Daryn Pakcyk, *Cyber-surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 79, 82 n.11 (2008) (crediting the DoubleClick decision as "one such rare instance of an informative and insightful court decision explaining Internet structure and programming").

[59] Tasker & Pakcyk, *supra* note 58, at 82 (noting that "attorneys who draft Internet agreements should understand the technical design and functioning of a particular web site to ensure that the provisions are drafted to cover the site's characteristics").

[60] 47 U.S.C. § 230(b)(1).

[61] *Id.* § 230(b)(2).

¶22 Under this "Good Samaritan" clause,"[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[62] The CDA explicitly stated that:

> [N]o provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.[63]

Pursuant to 47 U.S.C. § 230(e)(3), the CDA preempts any state or local law contrary to the "Good Samaritan" provision.[64]

¶23 In the first post-CDA decision, *Zeran v. America Online, Inc.*,[65] an anonymous poster placed a message on an America Online ("AOL") message board advertising T-shirts for sale.[66] The posting advertised "Naughty Oklahoma T-Shirts," promoting shirts featuring "offensive and tasteless slogans" related to the 1995 bombing of the Oklahoma City federal building.[67] Patrons interested in purchasing the shirts were to call "'Ken' at Zeran's home phone number in Seattle."[68] As a result of this posting, Zeran received many calls "comprised primarily of angry and derogatory messages, but also including death threats."[69] Zeran was not connected with the shirts or the ads, and AOL assured him that the post would be removed.[70]

¶24 In his suit, Zeran alleged negligence against AOL,[71] claiming that because he had alerted AOL to the hoax posting, "AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory

---

[62] 47 U.S.C.§ 230(c)(1). An "interactive computer service" includes "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id.* § 230(f)(2).
[63] *Id.* § 230(c)(2)(a).
[64] 47 U.S.C. § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").
[65] 129 F.3d 327 (4th Cir. 1997).
[66] *Id.* at 329.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.* at 328.

material."[72] The Fourth Circuit rejected Zeran's purported negligence claim because his pleading closely resembled a defamation action.[73] In analyzing the case as a defamation claim, the court cited the CDA and explained that section 230 created immunity against any action seeking to impose ISP liability for a third-party posting.[74] Thus, the court recognized AOL's defense and affirmed the District Court's granting of AOL's motion for judgment on the pleadings.[75]

¶25 While many post-CDA decisions have involved defamation claims, courts have applied CDA immunity to defendants in invasion of privacy cases. In *Parker v. Google, Inc.*, the plaintiff, an Internet publisher, claimed that his copyrighted work "29 Reasons Not to be a Nice Guy" had been partially copied and posted on the USENET without his permission.[76] The USENET is a global system of online bulletin boards wherein users can read, search and post messages, of which Google purchased an archive in 2000.[77] Parker asserted that Google invaded his privacy by creating an unauthorized biography of him whenever someone "Googled" his name into the search engine.[78] Furthermore, the complaint alleged that Google had been negligent as it continued to archive a website containing negative, defamatory statements even after Parker notified the site.[79] The District Court dismissed Parker's claims, including invasion of privacy, The Third Circuit affirmed the district court's decision to dismiss Parker's complaint.[80]

¶26 The question of whether the CDA applies to the whole spectrum of Prosserian invasion of privacy subcategories was addressed in *Doe v. Friendfinder Network, Inc*.[81] There, the plaintiff maintained that a profile containing a nude photo and a purported description of her proclivities was posted on the AdultFriendFinder.com online community website.[82] The

---

[72] *Id.* at 330.
[73] *Id.* at 332 ("Although Zeran attempts to artfully plead his claims as ones of negligence, they are indistinguishable from a garden variety defamation action.")
[74] *Zeran*, 129 F.3d at 330 (Section 230 "precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions-such as deciding whether to publish, withdraw, postpone or alter content-are barred.").
[75] *Id.* at 328–30.
[76] 242 Fed. App'x 833, 835 (3d Cir. 2007) (per curiam).
[77] *Id*.
[78] *Id.* at 838.
[79] *Id*.
[80] *Id.* at 840.
[81] 540 F. Supp. 2d 288 (D.N.H. 2008).
[82] *Id.* at 292.

Plaintiff sued the website for invasion of privacy, which she characterized as an infringement of her intellectual property rights. [83] Despite the defendant's attempts to take "special pains" to ensure posters' anonymity on the site, the profile photo nevertheless "reasonably identified" the plaintiff.[84]

¶27 The district court observed that CDA protections do not affect claims arising out of intellectual property law.[85] The defendant contended that allowing state-law intellectual property claims to survive CDA immunity would have a devastating impact on the Internet, as protecting individual intellectual property rights would be a cost of doing business online.[86] The court compromised with the defendants, reasoning that while the intellectual property exemption to CDA immunity has been established for misappropriation, commonly considered a "right of publicity" claim,[87] "[§230] applies with full force to the other invasion of privacy claims asserted in her complaint."[88]

¶28 The court found that the plaintiff demonstrated a sustainable claim for infringement of the right to publicity because the defendants used identifiable aspects of her persona in advertisements on other websites in order to increase the profitability of their site.[89] Thus, the court allowed the plaintiff to pursue the misappropriation claim, even though it dismissed the claims under the other Prosserian prongs of invasion of privacy.[90]

IV. THE ANONYMOUS INTERNET USER

¶29 The desire to publish anonymously predates the Internet, as anonymous authors enjoy the freedom to express themselves without fear of negative backlash. The Federalist Papers, for example, were published using pseudonyms.[91] Modern anonymous works, like those at issue in *Talley v. California*, continue to be protected by the courts. In that case, the Supreme Court voided a Los Angeles city ordinance forbidding the distribution of any handbill if it did not contain the name and address of its creator and its sponsor.[92] Such an identification requirement restricted the freedom to

---

[83] *Friendfinder*, 540 F. Supp. 2d at 298.
[84] *Id.*
[85] *Id.* (quoting 47 U.S.C. § 230(e)(2) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.")).
[86] *Id.* at 301–02.
[87] *Id.* at 302 (quoting Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1322 (11th Cir. 2006) ("[T]he right of publicity is [an] intellectual property right.")).
[88] *Id.* at 303.
[89] *Id.* at 304.
[90] *See id.* at 303.
[91] Talley v. California, 362 U.S. 60, 65 (1960).
[92] *Id.*

distribute information and thereby freedom of expression.[93] "Liberty of circulating is as essential to that freedom as liberty of publishing; indeed, without the circulation, the publication would be of little value."[94]

¶30 Many websites promote anonymity as a way for Internet users to have their voice on the web. Blogger, a site that facilitates independent blog creation, allows users to "[organize] the world's information from the personal perspective."[95] On Blogger, creators can design customized blogs on a limitless array of topics. The system, now owned by Google,[96] provides its customers with a free, user-friendly interface with which one can create a customized blog, discussing any topic the user desires.[97]

¶31 Though Blogger promotes communication and free expression, the site recognizes the boundary between freedom and abuse, and implements its content policy accordingly, pursuant to the CDA's purpose of promoting self-regulation.[98] The site prohibits bloggers from engaging in copyright infringement and publishing a third party's personal and confidential information.[99] The site also bars its users from misrepresenting themselves or appropriating another individual's identity, similar to the appropriation prong of invasion of privacy.[100] Upon being flagged, Blogger may respond by deleting the blog, disabling access to the author's Blogger or Google account, or in appropriate circumstances report the activity to law enforcement.[101]

¶32 Even though Blogger's content policies are admirable, the site's role as host to JuicyCampus calls into question whether it always enforces its established standards of appropriate conduct.[102] During its year-and-a-half operation, JuicyCampus administrators openly encouraged salacious discussion topics, with its motto being "Keep it Juicy."[103] Examples of such colorful threads included ones that sought the "biggest slut in each sorority"

---

[93] *Id* at 64.
[94] *Id.* (quoting Lovell v. City of Griffin, 303 U.S. 444, 452 (1938)).
[95] Blogger.com, The Story of Blogger, http://www.blogger.com/about (last visited Apr. 3, 2010).
[96] *Id.*
[97] Blogger.com, Blogger Features, http://www.blogger.com/features (last visited Apr. 3, 2010).
[98] Blogger.com, Content Policy, http://www.blogger.com/content.g (last visited Apr. 3, 2010).
[99] *Id.*
[100] *Id*.
[101] *Id*.
[102] JuicyCampus's connection to Blogger is established through its URL (http://juicycampus.blogspot.com/). The Blogger sites are hosted on Blogspot and are named accordingly. *See* Blogger Features, *supra* note 97.
[103] Young, *supra* note 18.

and the "gayest frat boys," with the discussions listing those who fit the labels.[104] Several state attorneys general investigated whether the site had committed consumer fraud by not adhering to its own guidelines for removing flagged posts, though site administrators claimed that it did comply with the established protocol.[105] Despite the complaints, threats of lawsuits and criminal investigations, the site continued to publish the "juicy" defamatory threads.[106]

¶33 Angry students finally disrupted JuicyCampus's operations by flooding the site with nonsense.[107] Students tried to clog the site with biblical passages, scientific articles, poetry verses, and even complete novels, causing the site to slow down.[108] Eventually, economic concerns and the lack of advertisement revenue led to the site's shutdown in February 2009.[109] The inability of courts and state agencies to sanction or shut down JuicyCampus due to the difficulty to prove the site's complicity in defamatory or fraudulent activities is quite troubling, and showcases the inherent limitations to government cyber-regulation resulting from the CDA immunity provision, to the benefit of sites that do not even abide by the spirit of the CDA to self-regulate.

¶34 Anonymous posting is also employed by reputable sites as a means of collecting important, potentially sensitive, information about institutions without fear of repercussions. Vault, for example, is used by job seekers wishing to benefit from the site's comprehensive database of company information, including insider information on salary scales, hiring procedures and company cultures.[110] Comments by employees are published anonymously both on the Vault website and in its print resources.[111] While Vault strives to preserve poster anonymity, the site does prohibit posting "any content or information that is unlawful, fraudulent, threatening, abusive, libelous, defamatory, obscene, harassing, misleading, false or otherwise objectionable, or that infringes on our or any third party's intellectual property or other proprietary rights."[112] Furthermore, as the information disclosed could be sensitive to the health of the company, non-

---

[104] *Id*.
[105] *Id*.
[106] *Id*.
[107] Bell, *supra* note 19.
[108] *Id*.
[109] Young, *supra* note 18.
[110] Vault.com, Mission, http://www.vault.com/ (follow "Mission' hyperlink) (last visited Nov. 3, 2009).
[111] Vault.com, Review Companies, http://www.vault.com (follow "Companies" hyperlink) (last visited Nov. 3, 2009).
[112] Terms of Use, *supra* note 16.

public information should not be posted.[113] If a post is flagged as violating the aforementioned rules, Vault considers editing or removing the post, or restricting the poster's access if necessary.[114]

¶35 Yet, Vault advises that, while specificity is required when discussing an employer, information about the author should not be sufficiently distinguishing so as to identify the individual.[115] Vault's privacy policy provides that the site may collect personally identifiable information, information that can be used to identify or contact this individual, upon registering to become a Vault member, purchasing a product on the site, using the site's personalized accounts, and participating in other activities related to the site.[116] Users who do decide to submit employer, profession or school reviews may be prompted for varied information depending on the review type, some of which may be personally identifiable.[117] However, credit card information is only collected if the user purchases the premium products or services solicited on the site.[118] Even credit cards are not always reliable in identifying the holder because prepaid credit cards can be purchased in most supermarkets, convenience stores, and pharmacies.[119] Thus, as the "personally identifiable" information is not easily verifiable and quite simple to fake, the sanctions imposed by Vault are nullified and the poster can create a new account to regain access.

¶36 The issue of disclosing non-public information is particularly pertinent when considering sites such as Yahoo! Finance, which provides accurate and up-to-date information on the health of firms and their outstanding securities as well as professional analysis and commentary by market experts on relevant financial topics.[120] Typing in a stock quote leads the user to an individualized page centered on the company.[121] On the

---

[113] *Id.*
[114] *Id.*
[115] Review Companies, *supra* note 111.
[116] Vault.com, Privacy Policy, http://www.vault.com (follow "Privacy Policy: Your Privacy Rights" hyperlink) (last visited Nov. 3, 2009). Personally identifiable information may include an individual's name, home address, email address, telephone number, text message address, email address, credit card information, age, gender and other demographic information. *Id.*
[117] *Id.*
[118] Vault.Com, Terms of Use, http://www.vault.com/ (follow "Terms of Use" hyperlink) (last visited Mar. 31, 2010).
[119] *See* Ryan Barrett, *Privacy through Prepaid Credit Cards*, Snarfed.org., Jan. 1, 2003.
[120] *See* Yahoo! Finance Homepage, http://finance.yahoo.com (last visited Nov. 4, 2009).
[121] Yahoo! Finance maintains individualized pages for countless firms; the pages vary in detail depending on the firm's market presence. To highlight the features available to users, the author used General Electric as a template. The author

company page, Yahoo! Finance includes essential investor tools such as a quote summary, interactive charts allowing the user to interpret the stock trends, news headlines from reputable news agencies,[122] company information including a firm profile and links to Securities and Exchange Commission, and industry and competitor comparisons.[123] Along with the professionally sponsored firm information, the site also maintains message boards wherein users may post comments about the firm.[124]

¶37 In a disclaimer, Yahoo! reminds site visitors that the message board is not affiliated with the company it concerns, and the messages posted thereon are solely the opinions of the users and cannot adequately substitute independent research, and should not be relied upon for the purpose of making investment decisions.[125] Yahoo! is adamant that users may not violate any laws through the site, including regulations set forth by the Securities and Exchange Commission, and such a violation may result in disclosure of account information if compelled by law to do so.[126] However, while the finance message boards warn that posters "never assume that [they] are anonymous and cannot be identified by [their] posts,"[127] it is not unimaginable that clever posters could frame their comments in such indistinguishable fashions as to remove any identifiable characteristics. Indeed, in order to become a Yahoo! member and thus qualify to post, a user need only provide a name, gender, birthday, country of origin, postal code, and email address.[128] Such details are not easily verifiable, calling into question the value of the site's promise to release account information if compelled to by law.

¶38 Yahoo! Finance provides a link to a page wherein the SEC succinctly explains the predicament faced by Internet investor sites.

---

typed "GE" into the "Get Quote" text box on the Homepage, *infra* note 196, and was redirected to the Yahoo Finance page for General Electric. http://finance.yahoo.com/q?s=GE (last visited Nov. 4, 2009) [hereinafter *General Electric Page*].

[122] The articles on Yahoo! Finance about General Electric originated from the Associated Press, Reuters, the Wall Street Journal, Barrons, Fox Business, and CNBC. Headlines for General Electric Company, http://finance.yahoo.com/q/h?s=GE (last visited Nov. 4, 2009).

[123] General Electric Page, *supra* note 121.

[124] Yahoo Finance, General Electric Message Board, http://messages.finance.yahoo.com/mb/GE (last visited Nov. 4, 2009).

[125] *Id*

[126] Yahoo.com, Terms of Service, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited Nov. 4, 2009).

[127] Yahoo! Finance, General Electric Message Board, *supra* note 124.

[128] Yahoo.com, Yahoo Registration, http://m.www.yahoo.com (follow "New here? sign up" link) (last visited Nov. 4, 2009).

Specifically, the agency advises Internet-reliant investors that finance bulletin boards are popular with fraudsters who overly promote certain firms, often by pretending to disclose "inside" information.[129] Alternatively, posters purporting to be unbiased investors who have merely conducted extensive research may actually be company insiders, large shareholders, or hired promoters.[130] In either event, it is difficult to know with whom one is dealing on those boards as they allow users to conceal their identity behind multiple aliases.[131] The prospect of a single poster utilizing multiple usernames is especially frightening as this can create an illusion of widespread interest in a little-known or otherwise undeserving firm or security.[132]

¶39 The issue of electronically disclosing material nonpublic information or fraudulent information in connection with investments in securities implicates SEC Rule 10b-5.[133] Rule 10b-5 provides that it is unlawful "to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading."[134] The SEC has used Rule 10b-5 to challenge corporate mismanagement, fraudulent liquidations, corporate misstatements and failures to disclose, unacceptable mergers, and insider trading.[135] The multitude of legal consequences, both civil and criminal, due to fraudulent disclosure and insider trading would presumably hold the bulletin board users accountable for their posts. Yet, securities officials and plaintiffs wronged by fraudulent investor advice cannot seek appropriate remedies if they are unable to identify the defendants.

---

[129] Securities and Exchange Commission, Internet Fraud: How to Avoid Internet Investment Scams, http://www.sec.gov/investor/pubs/cyberfraud.htm (last visited Nov. 5, 2009). A "pump-and-dump" scam is orchestrated by promoters who stand to profit by selling their shares after the stock price is pumped up by gullible investors. *Id.* This scam is typically associated with smaller companies because there is little or no public information available about the firm. *Id.*

[130] *Id.*

[131] *See id.*

[132] *See* Internet Fraud, *supra* note 129.

[133] 17 C.F.R. § 240.10b-5 (2008).

[134] *Id.* It would be illegal "[to] employ any device, scheme, or artifice to defraud" or "[to] engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security." *Id.*

[135] THOMAS LEE HAZEN, THE LAW OF SECURITIES REGULATION § 12.3[3] (6th ed. 2009) (explaining the circumstances in which Rule 10b-5 is used to seek civil remedies).

¶40 On October 3, 2008, an anonymous poster claimed on CNN's iReport.com[136] that Apple, Inc., CEO Steve Jobs had suffered a heart attack.[137] Though Apple denied the story, the company's stock price plummeted roughly 3 percent.[138] Eventually, the SEC identified the culprit as an 18-year-old who exhibited no apparent profit motivation from the market manipulation.[139] Regardless of this poster's intent, the disastrous consequences of posting false rumors seen here demonstrate the necessity for efficient accountability of all Internet stories that could have a material effect on the market, which is not possible if a user must only provide an email address to contribute even to a legitimate news site such as CNN.

¶41 Even if the individual user can supply a false name and email address when registering to post on an Internet bulletin board, presumably one could still be traced through the Internet Protocol (IP) address.[140] Tracing IP addresses is an established method utilized by law enforcement to identify and locate suspects in Internet-related crimes.[141] Yet, the danger of having one's IP address tracked by predators creates a demand for software with which users may disguise their IP addresses while browsing the Internet. For example, criminals employing spyware or malware software can see private chat sessions, intercept email communications, and log Web sites visit in order to acquire personal information.[142] Indeed, according to Anonymizer, 1.5 million Americans become victims of identity theft each year.[143] Anonymizer assures anonymous surfing by providing consumers with rotating anonymous IP addresses.[144] In doing so,

---

[136] http://www.ireport.com/.

[137] Greg Sandoval, *SEC Launches Probe into Phony Jobs Heart Attack Report*, CNET NEWS, Oct. 3, 2008, http://news.cnet.com/8301-1023_3-10058008-93.html (last visited Dec. 24, 2009).

[138] *Id.*

[139] *Id.*

[140] An IP address is an exclusive number all information technology devices (printers, routers, modems, etc.) use which allows them to communicate with each other on a computer network. What Is My IP, http://www.whatismyip.com/faq/what-is-an-ip-address.asp/ (last visited Nov. 5, 2009). IP addresses may either be assigned permanently, for an Email server, a business server or a home resident, or temporarily, from a pool of addresses (first come first serve) from your Internet Service Provider. *Id*.

[141] *See, e.g.*, Denise Dubie, *DNS Plays Role in Craigslist Killer Case*, NETWORK WORLD, Apr. 23, 2009, http://www.networkworld.com/news/2009/042309-craigslist-dns.html (explaining how network technology played a role in catching the killer and predicting that IP data identifying and locating criminals will expand its presence in the criminal investigation process).

[142] Anonymizer.com, Homepage, http://www.anonymizer.com (last visited Nov. 5, 2009).

[143] *Id.*

[144] *Id.*

Anonymizer strives to protect Internet users from invasion of privacy by intrusion or misappropriation. Anonymizer is not alone in its efforts to conceal Internet users' identity, as Tor[145] and the I2P Anonymous Network[146] provide similar services.

¶42 Yet, while Anonymizer's intent is noble, there is also the undeniable potential for abuse of an anonymous identity. Anonymizer prohibits users from utilizing its services to "invade the privacy of others" or "do anything illegal."[147] The company asserts its right to monitor use of the anonymous service as well as its prerogative to disclose communications in order to ensure compliance with the user agreement.[148] However, the site does not specify that it always monitors communications.[149] While the site uses filtering technology to intercept bulk emails and commercial emails, it is not clear that similar measures are in place to counter personal attacks on individuals' privacy.[150] Furthermore, as messages are sent anonymously, the recipient cannot report inappropriate behavior to the company, thereby denying it the chance to take the necessary measures.

V. THE COURTS' UNWILLINGNESS TO SHUT DOWN SITES ACCUSED OF OR COMPLICIT IN INVASION OF PRIVACY

¶43 The cases discussed *supra* demonstrate that courts continue to defer to the Internet companies' efforts to self-regulate as the firms contribute positively to the Internet's productivity. Many of the defendants in web-centered invasion of privacy and defamation litigation are widely used websites that contribute positively to society. For example, America Online—the corporation at issue in the 1997 *Zeran* case—was a leading

---

[145] Tor Anonymity Online, http://www.torproject.org (last visited Nov. 6, 2009). Tor is a network of virtual tunnels that allows people to improve their privacy and security on the Internet. Tor Overview, http://www.torproject.org/overview.html.en#overview (last visited Nov. 6, 2009).

[146] I2P Anonomous Network, Homepage, http://www.i2p2.de (last visited Nov. 6, 2009). "I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties." *Id.*

[147] Anonymizer.com, Terms of Use, http://www.anonymizer.com/company/legal/terms_of_use.html (last visited Nov. 5, 2009).

[148] *Id.*

[149] *See id.*

[150] *See id.*

Internet service provider, at one point boasting 30 million subscribers.[151] Google is a multiservice Internet conglomerate that provides users with a powerful search engine, email and instant messaging, office productivity functions, video sharing, and social networking.[152] Amazon, featured in the *Almeida* case,[153] is a web-based shopping venue, featuring everything from books to jewelry to home improvement supplies.[154] AdultFriendFinder, an adult matching and dating website, facilitates inter-personal relationships, albeit focusing on a concentrated audience.

¶44 Even sites that promote anonymous posting exhibit purposes that benefit society as a whole. Anonymizer provides its anonymity software in order to protect users from spyware and other means of tracking Internet movement and identity theft.[155] Vault, meanwhile, promotes open and honest discussion on institutions and industries so that students and professionals alike may formulate informed career decisions.[156] Yahoo! Finance encourages the dissemination of financial information among relatively amateur investors to supplement the professional commentaries in order to gauge the health of their investments.[157]

¶45 The aforementioned sites and their anonymity components provide ample opportunity for users to engage in egregious invasions of privacy. However, as the sites reserve the right to monitor for and remove inappropriate content, they satisfy the CDA "Good Samaritan" provision and thus are exempt from civil liability.[158] Furthermore, while "John Doe" subpoenas could be served on Yahoo! and Vault to produce the poster's personal information, it is quite possible that the individual provided fraudulent information. An IP address would be a more precise method of ascertaining information about the poster. However, anonymous proxy software provided by Anonymizer, Tor, or I2P disguises the IP address from investigators. Alternatively, the plaintiff could direct the "John Doe" subpoenas at the anonymous software provider. In fact, these sites could be concentrated treasure troves of information on anonymous posters, sought by private and government parties alike. However, these sites could be capable of hiding the user's identity if they employed a technique akin to

---

[151] Catherine Holahan, *Will Less Be More for AOL?*, BUS. WK., July 31, 2006, http://www.businessweek.com/technology/content/jul2006/tc20060731_168094.htm (last visited Nov. 6, 2009).
[152] *See* Google Homepage, http://www.google.com/ (last visited Nov. 6, 2009).
[153] *See generally* Almeida v. Amazon.com, Inc., 456 F.3d 1316 (11th Cir. 2006).
[154] *See* Amazon Homepage, http://www.amazon.com/ (last visited Nov. 6, 2009).
[155] *See* Anonymizer Homepage, *supra* note 142.
[156] *See* Vault.com, Mission, *supra* note 110.
[157] *See* General Electric Page, *supra* note 121.
[158] *See* 47 U.S.C. § 230(c) (2006).

spread spectrum technology, and scattered the information across the Internet.[159]

¶46 When the plaintiff's injury originated with an Internet user employing anonymity software, the plaintiff could subpoena the personal information from the Anonymizer site. Yet, all Internet users, even the defendant, have an expectation of privacy. In addition to information collected upon purchasing products, Anonymizer gathers information on site visitors including IP addresses, browser type and language, and the date of visit.[160] Aside from consensual disclosure, Anonymizer releases usage information if disclosure is "reasonably necessary to satisfy any applicable law, regulation, legal process or enforceable governmental request," or to "protect against imminent harm to the rights, property or safety of Anonymizer, [its] customers or the public."[161] The "imminent harm" requirement for voluntary release could be problematic, as the site is responsible for determining what is imminent. Furthermore, specifying "imminence" would not likely give the proper authorities ample opportunity to mount an appropriate response. In the context of self-defense, courts have limited "imminence" to "'reasonably probable,' not merely possible,"[162] and refer to a "'present'" threat as opposed to a future one.[163] Thus, while striving to preserve its users' privacy, Anonymizer only presents opportunities for subsequent remedial measures, while limiting the window for preventative ones.

¶47 The "reasonably necessary" standard undoubtedly includes responding affirmatively to "John Doe" subpoenas, and is consistent with a recent ruling by the Court of Appeals for the District of Columbia Circuit, in which the court articulated a five-step test to be applied when presented with a motion to quash or enforce such a subpoena.[164] The court should first ensure that the plaintiff has "adequately pleaded the elements of the

---

[159] Spread spectrum is "wireless communications technology that scatters data transmissions . . . in a pseudorandom pattern. Spreading the data across the frequency spectrum greatly increases the bandwidth, and it also makes the signal resistant to noise, interference, and snooping." CNET Reviews, CNET Glossary: Spread Spectrum, http://reviews.cnet.com/4520-6029_7-5958697-1.html/ (last visited April 13, 2010).

[160] Anonymizer.com, Privacy Policy, http://www.anonymizer.com/company/legal/privacy_policy.html (last visited Nov. 6, 2009). Anonymizer is the most commercial of the three anonymity services I have identified, and sets forth the most thorough policy.

[161] *Id.*

[162] People v. Robinson, 872 N.E.2d 1061, 1076 (Ill. App. Ct. 2007) (quoting State v. Payne, 7 S.W.3d 25, 28 (Tenn. 1999)).

[163] *Robinson*, 872 N.E.2d at 1076 (quoting Kessler v. State, 850 S.W.2d 217, 222 (Tex. App. 1993)).

[164] *See* Solers, Inc. v. Doe, 977 A.2d 941, 954 (D.C. 2009).

claim."[165] Then, the court should demand reasonable efforts on the part of the Internet firm "to notify the anonymous defendant that the complaint has been filed and the subpoena has been served," and possibly "delay further action for a reasonable time to allow the defendant an opportunity to file a motion to quash" the subpoena.[166] The plaintiff must present evidence "creating a genuine issue of material fact on each element of the claim that is within its control," or all elements not dependent on knowing the defendant's identity.[167] In evaluating this evidence, the court should determine whether the information sought is vital to enable the plaintiff to proceed with the lawsuit.[168] This test provides insight into the steep threshold that private and government plaintiffs must overcome to gain access to information that users shared with the utmost expectation of privacy. The consistency between this court's standard for enforcing "John Doe" subpoenas and Anonymizer's own protocols reinforces the inference that a court would comply with the CDA and defer accordingly to its self-regulatory policy.

¶48 Indeed, the Internet's global scope creates situations in which anonymity is necessary to avoid undue risk and possible bodily harm to users. Regimes that rigidly limit the free dissemination of information often seek user information from Internet companies, and those firms that rely on continued service in that country comply to ensure future business.[169] For example, Google, Microsoft, and Yahoo! have faced scrutiny for helping China monitor and censor content.[170] Yahoo! was even accused of exposing a Chinese journalist who sent a summary of Communist Party communications to a foreign website via Yahoo!'s email service.[171] The danger faced by Internet users in various countries necessitates the existence of "anonymizing" software, and would justify barring any civil actions brought against the vendors in American court under section 230 of the CDA.

¶49 American courts have in the past supported actions to shut down Internet companies that come under fire and are not shown to serve a "legitimate" purpose. The Napster case[172] is one example of this judicial

---

[165] *Id.*
[166] *Id.*
[167] *Id.* at 954-55.
[168] *Id.* at 954.
[169] Joseph Kahn, *Yahoo Helped Chinese to Prosecute Journalist*, N.Y. TIMES, Sept. 8, 2005, http://www.nytimes.com/2005/09/07/business/worldbusiness/07iht-yahoo.html.
[170] *Id.*
[171] *Id.*
[172] *See generally* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

selective Darwinism. Napster facilitated file-sharing of MP3 audio files, allowing users to search the MP3 music files stored on other users' computers and transfer copies of the contents of other users' MP3 files from one computer to another.[173] The recording company plaintiffs alleged that Napster users engaged in the wholesale reproduction and distribution of copyrighted works, all constituting direct infringement of copyright law,[174] and that Napster facilitated the infringements.[175] Although Napster contended that the users' actions constituted fair use of the material,[176] the Ninth Circuit could not find a valid fair use defense available to users.[177] Furthermore, the plaintiffs demonstrated a likelihood of success with regards to the contributory copyright infringement claim.[178] The court also dismissed Napster's proposed compulsory royalty as an "easy out" for the embattled company, and reasoned that the imposition of such a device would destroy the plaintiffs' ability to control their intellectual property.[179] The injunction issued by the District Court remained in place and Napster was prohibited from conducting its business.[180]

¶50 However, judicial action has not been shown to provide absolute solutions when confronting legal issues in cyberspace. Even though the court enjoined Napster from hosting its file-sharing operations and infringing copyright law, new sites have emerged since Napster, engage in similar activities, and still persist. For instance, BitTorrent is an Internet-based protocol allowing users to download files quickly by uploading parts of them at the same time.[181] While this program does have a strict copyright policy,[182] the fragmented nature of the file sharing would complicate an infringement complaint. The justice system's inability to act decisively was evident in the JuicyCampus case, where state officials were so unacceptably slow at demonstrating the raucous site's violations of the CDA that students were forced to shut down the site by essentially spamming the site.[183]

---

[173] *Id.* at 1011.
[174] *See* 17 U.S.C. §§ 106(1), 106(3) (2006).
[175] *Napster*, 239 F.3d at 1011.
[176] *Id.* at 1014.
[177] *Id.* at 1019.
[178] *Id.* at 1022.
[179] *Id.* at 1028-29.
[180] *See id.* at 1029.
[181] BitTorrent.com, What is BitTorrent?, http://www.bittorrent.com/btusers/what-is-bittorrent (last visited Nov. 6, 2009).
[182] BitTorrent.com, Copyright Policy, http://www.bittorrent.com/legal/copyright-policy (last visited Nov. 6, 2009) ("BitTorrent does not permit copyright infringing activities on its websites and will, if properly notified that files infringe a copyright, remove or disable access to such files.").
[183] *See* Young, *supra* note 18; *see also* Bell, *supra* note 19.

¶51 If reputable websites with ample public support are immune from liability pursuant to the CDA, the correct method of assigning liability may lie with targeting the individual user. To ensure that a potential defendant's privacy is protected, a burden of reasonable certainty of misuse, reasonable harm, and time elapsed since the initial reporting should be the threshold showing to retrieve personal information for service. That is, a plaintiff should show that a reasonable person would conclude that the defendant misused the Internet service to perpetrate the tort. Also, a plaintiff should demonstrate a reasonable person would be harmed or offended by the conduct. The time variable gives the companies ample time to self-regulate before involving an outside body. This triple-pronged test resembles the *Solers* test,[184] and implicates the spirit of the CDA to encourage self-regulation, while offering injured plaintiffs a judicial option if private efforts fail.

VI. THE SOLUTION: VERIFICATION FOR ALL USERS

¶52 If the courts are not going to hold websites accountable for the damaging posts of anonymous users, and judicial focus shifts onto the posters, then one possible solution would be to have the posters confidentially lodge and verify their identity with an authentication service. This would hold users accountable for their posts and would present opportunity for service by plaintiffs. The verification system should be similar to the model employed by VeriSign. VeriSign, Inc. is a leading provider of digital trust services that enable Web site owners, enterprises, communications service providers, electronic commerce, and individuals to engage in secure digital commerce and communications.[185] The company's identity and authentication services provide web-based companies with secure fraud detection and authentication for protecting the online identities of consumers, business partners, and employees.[186] The Secure Sockets Layer (SSL) certification services enable secure commerce, communications, and interactions by providing encryption and authentication services to Web sites, intranets, and extranets.[187]

¶53 All sites that allow posters to publish comments anonymously should require that users register with an independent identity verification service, so that the actions associated with the assigned anonymous identity

---

[184] *See* Solers, Inc. v. Doe, 977 A.2d 941, 954-55 (D.C. 2009).
[185] Fundinguniverse.com, VeriSign, Inc. Company History, http://www.fundinguniverse.com/company-histories/VeriSign-Inc-Company-History.html (last visited Nov. 6, 2009).
[186] Verisign.com, Company Information, http://www.verisign.com/corporate/information/index.html (last visited Nov. 6, 2009).
[187] *Id.*

may be tracked and traced back to the individual. This program would be just as secure as Anonymizer and facilitate an informed expectation of privacy. Many Internet users are not aware that their activities online can be tracked by their IP address.[188] However, upon registering for an anonymous identity, the verification program would advise users of the appropriate expectation of privacy under this new regime. Specifically, a disclaimer would inform users that, while harmless web browsing would not trigger disclosure, actions violating the law could lead to their identity being uncovering and released to the proper authorities.

¶54 In order to register for an anonymous identity, the service should require a valid name, address, birthday as verification for age-sensitive sites, driver's license number (or equivalent thereof), and city of birth. Furthermore, users should have the option to enter credit card information at this point to use this system for universal payments, similar to PayPal. The credit card information should be used or released solely for the purpose of facilitating purchases. However, the card may not be prepaid. Though a valid social security number is the most accurate form of identification, the consequences of losing such data should be quite disastrous for the user. There should understandably be trepidation concerning sharing such sensitive information over the Internet. However, any data provided should be encrypted and presumably safe from hackers trying to procure the private information. This security is consistent with the ECPA's purpose of protecting electronically stored communications.[189]

¶55 The proposed identity verification system should be independently run. It should not be a government entity since the global nature of the Internet should pose problematic jurisdictional questions over which governmental body should be responsible for management, maintenance and security. Furthermore, an Internet poster interested in anonymity is likely seeking to avoid government attention, and should be reluctant to input personal information into a government database. The verification program should also be independent of the websites requiring registration,

---

[188] *See* Kelly Martin, *Privacy and Anonymity*, SECURITYFOCUS, Feb. 14, 2006, http://www.securityfocus.com/columnists/386 (explaining that while "only about a third of the public even knows what spyware is; . . . as broadband connections have become inexpensive and pervasive, we are increasingly being tracked by our IP addresses at home. If you have high speed Internet at home, odds are your IP address is relatively static now - cable and DSL modems are often assigned the same IP address for up to a year. Website owners can track your repeat visits much more easily - what time you arrived, how long you stayed, and how often you come back.").

[189] *See* 18 U.S.C. § 2701(a) (2006) (asserting that it is illegal to obtain, alter, or otherwise interfere with authorized access to a wire or electronic communication while it is in electronic storage).

so that these websites should not be hampered or burdened by additional self-regulation. The sites' regulatory efforts should be solely focused on ensuring that they delete content flagged as an invasion of privacy or defamatory. This initiative also supports the spirit of the CDA and its interest of promoting Internet usage as users should feel more secure in their posts, and the sites should be free to allocate their resources towards further progress and innovation.

¶56 Although the websites should not be responsible for collecting user data, they should have easy access to it. In a civil suit, the plaintiff should serve the website with a "John Doe" subpoena, assuming the threshold derived in Part V could be met. The site should comply with the subpoena, and provide the necessary information. The easily accessible data saves all parties from the costs of suing the website directly, especially if the court should ultimately going to dismiss the claim as a result of CDA immunity. The websites should have no reason to access the verification information unless served with a valid subpoena. Rather, a given website should only record the anonymous identity assigned to that user. Thus, the user should not have to procure anonymous proxy software from Anonymizer, Tor, or the I2P Anonymous Network. Transaction costs are minimized both in setting up multiple Internet accounts and in tracking down and contacting the proxy service.

¶57 Though this subpoena structure is intended for use in private actions, government investigators should presumably procure Internet user information in the same fashion. While this identity-verification project should not be government-controlled, it should be initiated through legislative mandate and subject to rigorous regulatory oversight.

¶58 Identity verification as described in this iBrief should only apply within the United States, to American Internet domains. As demonstrated above, it is quite possible that global anonymous proxies that disguise IP numbers serve a legitimate and necessary purpose in countries with strict Internet content restrictions in place. Indeed, it is impossible at this stage to consider how this proposed identity-verification software should be adopted in countries where strict censorship regimes hinder the free dissemination of information, and where state officials should closely monitor the identities and movements of Internet users.

CONCLUSION

¶59 Anonymous posting on Internet websites and the rampant invasions of privacy committed by unconcerned Internet users is alarming. Yet, in trying to identify the parties, the plaintiff must face the formidable task of overcoming CDA immunity. At the same time, courts and politicians must consider the defendant's expectation of privacy in posting anonymously

online. The heightened standard for procuring subpoenas described here seeks to serve as a compromise for the conflicting privacy interests. However, the most effective way, both from an economic and a legal standpoint, to manage Internet anonymity would be to develop a centralized, independent identity-verification system. This model would instill greater consumer confidence in the Internet, and would abide by the spirit of the CDA and promote the continued growth of the World Wide Web into the future.